IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) An apparatus for encrypting block data of a first bit length ~~size~~ comprising:

encrypting sections connected in series, each of the encrypting sections comprising,

first units each configured to randomize first subblock data of a second bit length ~~size~~ which are obtained by dividing the block data of the first bit length ~~size~~, and

a second unit configured to receive plural items of the randomized first subblock data output from the first units, the received plural items of the randomized first subblock data being of the first bit length, to diffuse the received plural items of the randomized first subblock data of the first bit length ~~a group of data which is of the first size and is output from the first units~~ and to supply a result of diffusion to first units in a succeeding encrypting section, and wherein ~~the first units and the second unit are configured to connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit~~ each of the first units comprises

first subunits each configured to randomize second subblock data of a third bit length which are obtained by dividing the first subblock data of the second bit length,

a second subunit configured to receive plural items of the randomized second subblock data output from the first subunits, the received plural items of the randomized second subblock data being of the second bit length and to diffuse the received plural items of the randomized second subblock data of the second bit length, and

third subunits configured to receive the diffused second subblock data of the second bit length which is output from the second subunit and each configured to randomize the second subblock data of the third bit length, and

wherein any one of the first subunits is connected to any one of the first subunits in the succeeding encrypting section via at least two paths.

2 (Canceled).

3 (Canceled).

4. (Currently Amended) An apparatus for encrypting block data of a first bit length ~~size~~, the apparatus comprising:

encrypting sections connected in series, each of the encrypting sections comprising,

first nonlinear transformation units each configured to perform a nonlinear transformation process for first subblock data of a second bit length ~~size~~ which are obtained by dividing the block data of the first bit length ~~size~~, and

a first linear diffusion unit configured to receive plural items of the processed first subblock data output from the first nonlinear transformation units, the received plural items of the processed fist subblock data being of the first bit length, to perform a linear diffusion process for the received plural items of the processed first subblock data of the first bit length ~~a linear diffusion process for a group of the first subblock data which is of the first size and is output from the first nonlinear transformation units~~ and to supply a result of the linear diffusion process to first nonlinear transformation units in a succeeding encrypting section,

wherein each of the first nonlinear transformation units comprises,

second nonlinear transformation units each configured to perform a nonlinear transformation process for second subblock data of a third bit length ~~size~~ which are obtained by dividing the first subblock data of the second bit length ~~size~~, ~~and~~

a second linear diffusion unit configured to receive plural items of the processed second subblock data output from the second nonlinear transformation units, the received plural items of the processed second subblock data being of the second bit length and to perform a linear diffusion process for ~~a group of~~ the received plural items of the processed second subblock data, ~~which is of the third size and is output from the second nonlinear transformation units, and~~

third nonlinear transformation units configured to receive the processed second subblock data of the second bit length which is output from the second linear diffusion unit and each configured to perform a nonlinear transformation process for second subblock data of the third bit length,

wherein ~~the first nonlinear transformation units, the first linear diffusion unit, the second nonlinear transformation units, and the second linear diffusion unit are configured to connect at least one input bit terminal of the first nonlinear transformation units to one input bit terminal of the corresponding first nonlinear transformation units~~ any one of the second nonlinear transformation units is connected to any one of the second nonlinear transformation units in the succeeding encrypting section via at least two paths.

5. (Canceled)

6. (Canceled)

7 (Canceled).

8. (Currently Amended) The apparatus according to claim 4, wherein the ~~block data~~ first bit length is 128 bits ~~in length~~, ~~each of the first subblock data~~ the second bit length is 32

bits, ~~in length~~ and the third bit length is 8 bits.

9. (Currently Amended) The apparatus according to claim 4, wherein the first linear diffusion unit and the second linear diffusion unit are [[is]] implemented by hardware.

10. (Currently Amended) The apparatus according to claim 9, wherein an input-output characteristic of the first linear diffusion unit and the second linear diffusion unit are [[is]] based on multiplication in a Galois field.

11. (Currently Amended) The apparatus according to claim [[5]] 4, wherein the first linear diffusion unit and the second linear diffusion unit are [[is]] implemented by software.

12. (Currently Amended) An apparatus for encrypting block data of 128 bits, the apparatus comprising:

encrypting sections connected in series, each of the encrypting sections including,

four first nonlinear transformation units each configured to perform a nonlinear transformation process for first subblock data of 32 bits which are obtained by dividing the block data, and

a first linear diffusion unit configured to receive plural items of the processed first subblock data output from the four first nonlinear transformation units, to perform a linear diffusion process ~~using a maximum distance separable matrix~~ for ~~a group of~~ the received plural items of the processed first subblock data of 32 bits ~~the first subblock data of 128 bits output from the four first nonlinear transformation units~~ and to supply a result of the linear diffusion process to four first nonlinear transformation units in a succeeding encrypting section;

a key addition unit which adds key data of 128 bits to output data of 128 bits from the encrypting section of a last stage,

wherein an encrypting section of the last stage comprises four nonlinear transformation units each configured to perform a nonlinear transformation process for the first subblock data of 32 bits,

wherein each of the first nonlinear transformation units includes stage sections, each stage section including,

four second nonlinear transformation units each configured to perform a nonlinear transformation process for second subblock data of 8 bits which are obtained by dividing the first subblock data,

a second linear diffusion unit configured to receive plural items of the processed second subblock data output from the four second nonlinear transformation units, the received plural items of the processed second subblock data being 32 bits in length, and to perform a linear diffusion process for ~~a group of~~ the received plural items of the processed second subblock data, ~~of 32 bits output from the second nonlinear transformation units, and~~

third nonlinear transformation units configured to receive the processed second subblock data which is output from the second linear diffusion unit and each configured to perform a nonlinear transformation process for second subblock data being 8 bits in length, and

an adder for adding a key to four second subblock data of 8 bits input to the four second nonlinear transformation units,

wherein a stage section of the last stage comprises four second nonlinear transformation units each configured to perform a nonlinear transformation process for the second subblock data;

wherein ~~the first nonlinear transformation units, the first linear diffusion unit, the second nonlinear transformation units, and the second linear diffusion unit are configured to connect at least one input bit terminal of the first nonlinear transformation units to one input bit terminal of the corresponding first nonlinear transformation units~~ any one of the four second nonlinear transformation units is connected to any one of the four second nonlinear transformation units in the succeeding encrypting section via at least two paths, and

wherein each of the four first nonlinear transformation units divides input data of 32 bits into eight groups of data of 4 bits which are formed of extracting the input data by every 8 bits, and the first linear diffusion unit comprises eight subunits each subunit receiving corresponding four groups of data of 4 bits output from the four first nonlinear transformation units, performing a 4×4 matrix operation based on multiplication over a Galois field $GF(2^4)$

for the received four groups of data of 4 bits, and outputting four groups of data of 4 bits to corresponding four first nonlinear transformation units of the succeeding encrypting section.

13. (Currently Amended) An apparatus for encrypting block data of 64 bits, the apparatus comprising:

encrypting sections connected in series, each of the encrypting sections including,

two first nonlinear transformation units each configured to perform a nonlinear transformation process for first subblock data of 32 bits which are obtained by dividing the block data, and

a first linear diffusion unit configured to receive plural items of the processed first subblock data output from the two first nonlinear transformation units, perform a linear diffusion process ~~using a maximum distance separable matrix~~ for ~~a group~~ the received plural items of the processed first subblock data of 32 bits ~~of the first subblock data, of 64 bits output from the two first nonlinear transformation units~~ and to supply a result of the linear diffusion process to two first nonlinear transformation units in a succeeding encrypting section;

a key addition unit which adds key data of 128 bits to output data of 64 bits from the encrypting section of a last stage,

wherein an encrypting section of the last stage comprises two nonlinear transformation units each configured to perform a nonlinear transformation process for the first subblock data of 32 bits,

wherein each of the first nonlinear transformation units includes stage sections, each stage section including,

four second nonlinear transformation units each configured to perform a nonlinear transformation process for second subblock data of 8 bits which are obtained by dividing the first subblock data,

a second linear diffusion unit configured to receive plural items of the processed second subblock data output from the four second nonlinear transformation units, the received plural items of the processed second subblock data being 32 bits in length, and to perform a linear diffusion process for ~~a group of~~ the received plural items of the processed second subblock data being 32 bits in length, ~~the second subblock data of 32 bits output from the second nonlinear transformation units, and~~

third nonlinear transformation units configured to receive the processed second subblock data which is output from the second linear diffusion unit and each configured to perform a nonlinear transformation process for second subblock data being 8 bits in length, and

an adder for adding a key to four second subblock data of 8 bits input to the four second nonlinear transformation units,

wherein a stage section of the last stage comprises four second nonlinear transformation units each configured to perform a nonlinear transformation process for the second subblock data,

wherein ~~the first nonlinear transformation units, the first linear diffusion unit, the second nonlinear transformation units, and the second linear diffusion unit are configured to connect at least one input bit terminal of the first nonlinear transformation units to one input bit terminal of the corresponding first nonlinear transformation units~~ any one of the four second nonlinear transformation units is connected to any one of the four second nonlinear transformation units in the succeeding encrypting section via at least two paths, and

wherein each of the two first nonlinear transformation units divides input data of 32 bits into eight groups of data of 4 bits which are formed of extracting the input data by every 8 bits, and the first linear diffusion unit includes eight subunits each subunit receiving corresponding two groups of data of 4 bits output from the two first nonlinear transformation units, performing a 2×2 matrix operation based on multiplication over a Galois field $GF(2^4)$ for the received two groups of data of 4 bits, and outputting two groups of data of 4 bits to corresponding two first nonlinear transformation units of the succeeding encrypting section.

14. (Currently Amended) A method for encrypting block data of a first ~~size~~ bit length comprising:

~~randomizing each of first subblock data of a second size which are obtained by dividing the block data of the first size;~~

~~diffusing a group of the randomized data of the first size; andrepeating the randomizing, the recievint, and the diffusing,~~

randomizing first subblock data of a second bit length which are obtained by dividing the block data of the first bit length;

receiving plural items of the randomized first subblock data, the received plural items of the randomized first subblock data being of the first bit length;

diffusing the received plural items of the randomized first subblock data of the first bit length; and

repeating the randomizing, the receiving, and the diffusing,

wherein at least one bit input to the randomizing operation is transmitted to the next randomizing operation via at least two paths.

15. (Currently Amended) An article of manufacture comprising a computer readable medium including a computer program embodied therein, the computer program comprising:

~~computer readable program code means for causing a computer to randomize each of first subblock data of a second size which are obtained by dividing plaintext block data of a first size;~~

~~computer readable program code means for causing a computer to diffuse a group of the randomized data of the first size; and~~

~~computer readable program code means for causing a computer to repeat the randomizing and the diffusing, wherein at least one bit input to the randomizing operation is transmitted to the next randomizing operation via at least two randomizing and diffusing paths~~

computer readable program code means for causing a computer to randomize first subblock data of a second bit length which are obtained by dividing the block data of a first bit length;

computer readable program code means for causing a computer to receive plural items of the randomized first subblock data, the received plural items of the randomized first subblock data being of the first bit length;

computer readable program code means for causing a computer to diffuse the received plural items of the randomized first subblock data of the first bit length; and

computer readable program code means for causing a computer to repeating the randomizing, the receiving, and the diffusing,

wherein at least one bit input to the randomizing operation is transmitted to the next randomizing operation via at least two paths.

16. (Currently Amended) An apparatus for decrypting encrypted block data of a first bit length, the apparatus comprising:

decrypting sections connected in series, each of the decrypting sections comprising,

first units each configured to randomize first subblock data of a second bit length ~~size~~ which are obtained by dividing encrypted block data of the first bit length ~~size~~, and

a second unit configured to receive plural items of the randomized first subblock data output from the first units, the received plural items of the randomized first subblock data being of the first bit length, to diffuse the received plural items of the randomized first subblock data of the first bit length ~~a group of data which is of the first size and is output from the first units~~ and to supply a result of diffusion to first units in a succeeding ~~encrypting~~ decrypting section, and wherein ~~the first units and the second unit are configured to connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit~~ each of the first units comprises

first subunits each configured to randomize second subblock data of a third bit length which are obtained by dividing the first subblock data of the second bit length,

a second subunit configured to receive plural items of the randomized second subblock data output from the first subunits, the received plural items of the randomized second subblock data being of the second bit length and to diffuse the received plural items of the randomized second subblock data of the second bit length, and

third subunits configured to receive the diffused second subblock data of the second bit length which is output from the second subunit and each configured to randomize the second subblock data of the third bit length, and

wherein any one of the first subunits is connected to any one of the first subunits in the succeeding ~~encrypting~~ decrypting section via at least two paths.

17. (Currently Amended) A method for decrypting encrypted block data of a first bit length ~~size~~, the method comprising:

~~randomizing first subblock data of a second size which are obtained by dividing the encrypted block data of the first size;~~

~~diffusing a group of the randomized data of the first size; and~~

~~repeating the randomizing and the diffusing,~~

randomizing first subblock data of a second bit length which are obtained by dividing the block data of the first bit length;

receiving plural items of the randomized first subblock data, the received plural items of the randomized first subblock data being of the first bit length;

diffusing the received plural items of the randomized first subblock data of the first bit length; and

repeating the randomizing, the receiving, and the diffusing,

wherein at least one bit input to the randomizing operation is transmitted to the next randomizing operation via at least two paths.

18. (Currently Amended) An article of manufacture comprising a computer readable medium including a computer program embodied therein, the computer program comprising:

~~computer readable program code means for causing a computer to randomize first subblock data of a second size which are obtained by dividing encrypted block data of a first size;~~

~~computer readable program code means for causing a computer to diffuse a group of the randomized data of the first size; and~~

~~computer readable program code means for causing a computer to repeat the randomizing and the diffusing,~~

computer readable program code means for causing a computer to randomize first subblock data of a second bit length which are obtained by dividing the block data of a first bit length;

computer readable program code means for causing a computer to receive plural items of the randomized first subblock data, the received plural items of the randomized first subblock data being of the first bit length;

computer readable program code means for causing a computer to diffuse the received plural items of the randomized first subblock data of the first bit length; and

computer readable program code means for causing a computer to repeating the randomizing, the receiving, and the diffusing,

wherein at least one bit input to the randomizing operation is transmitted to the next randomizing operation via at least two paths.